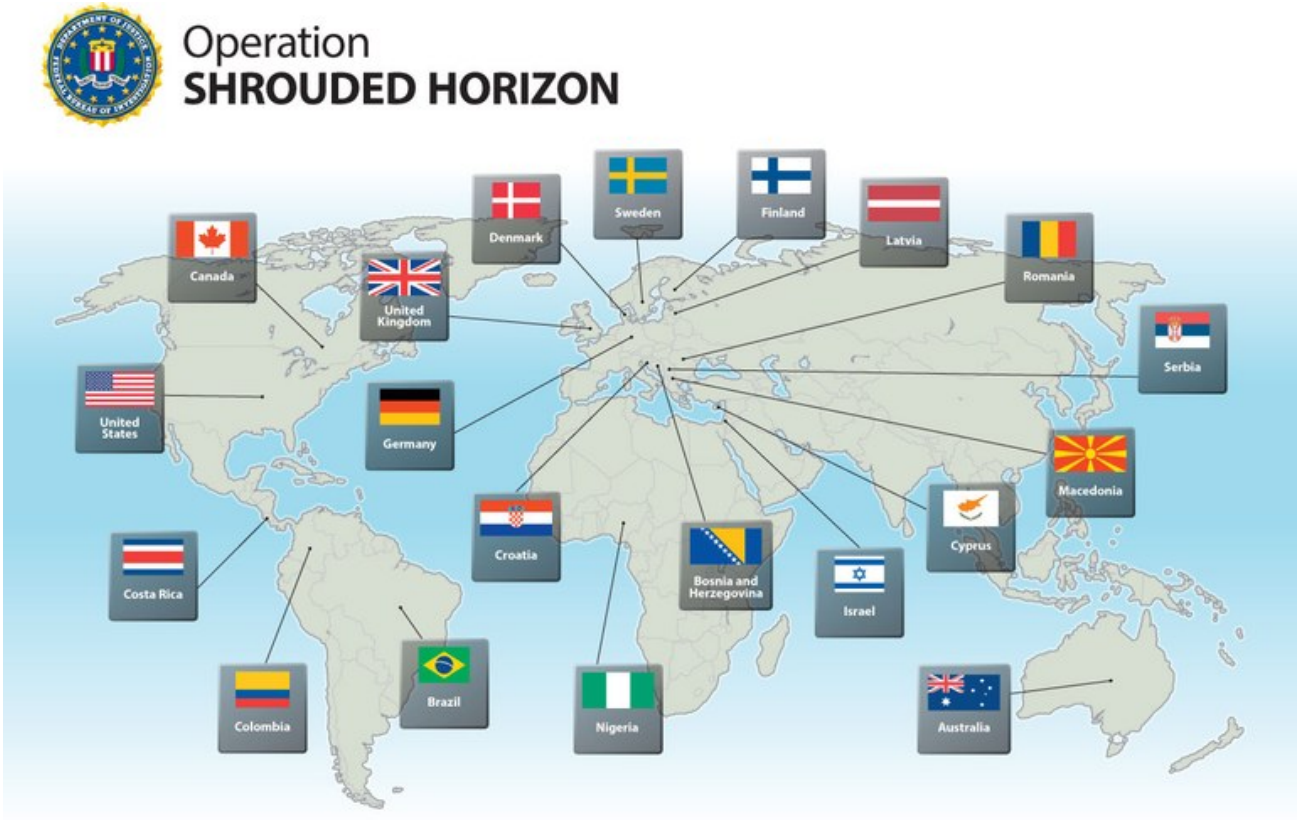
July 15, 2015

Cyber Criminal Forum Taken Down

Members Arrested in 20 Countries



The Shrouded Horizon investigation against the Darkode cyber criminal forum involved law enforcement agencies in 20 countries.

It was, in effect, a one-stop, high-volume shopping venue for some of the world's most prolific cyber criminals. Called Darkode, this underground, password-protected, online forum was a meeting place for those interested in buying, selling, and trading malware, botnets, stolen personally identifiable information, credit card information, hacked server credentials, and other pieces of data and software that facilitated complex cyber crimes all over the globe.

Unbeknownst to the operators of this invitation-only, English-speaking criminal forum, though, the FBI had infiltrated this communication platform at the highest levels and began collecting evidence and intelligence on Darkode members.

And today, the Department of Justice and the FBI—with the assistance of our partners in 19 countries around the world—announced the results of Operation Shrouded Horizon, a multi-agency investigation into the Darkode forum. Among those results were charges, arrests, and searches involving 70 Darkodemembers and associates around the world; U.S. indictments against 12 individuals associated with the forum, including its administrator; the serving of several search warrants in the U.S.; and the Bureau's seizure of Darkode's domain and servers.

The above message was displayed on the Darkode homepage after the FBI seized its web domain and servers.

Said FBI Deputy Director Mark Giuliano, "Cyber criminals should not have a safe haven to shop for the tools of their trade, and Operation Shrouded Horizon shows we will do all we can to disrupt their unlawful activities."

During the investigation, the Bureau focused primarily on the Darkode members responsible for developing, distributing, facilitating, and supporting the most egregious and complex cyber criminal schemes targeting victims and financial systems around the world, including in the United States.

The Darkode forum, which had between 250-300 members, operated very carefully—not just anyone could join. Ever fearful of compromise by law enforcement, Darkode administrators made sure prospective members were heavily vetted.

Similar to practices used by the Mafia, a potential candidate for forum membership had to be sponsored by an existing member and sent a formal invitation to join. In response, the candidate had to post an online introduction—basically, a resume—highlighting the individual's past criminal activity, particular cyber skills, and potential contributions to the forum. The forum's active members decided whether to approve applications.

Once in the forum, members—in addition to buying and selling criminal cyber products and services—used it to exchange ideas, knowledge, and advice on any number of cyber-related fraud schemes and other illegal activities. It was almost like a think tank for cyber criminals.

What's the significance of this case, believed to be the largest-ever coordinated law enforcement effort directed at an online cyber criminal forum? In addition to shutting down a major resource for cyber criminals, law enforcement infiltrated a closed criminal forum—no easy task—to obtain the intelligence and evidence needed to identity and prosecute these criminals. And this action paid off with a treasure trove of information that ultimately led to the dismantlement of the forum and law enforcement actions against dozens of its worst criminal members around the world.

The case was led by the FBI's Pittsburgh Field Office, with assistance from our offices in Washington, San Diego, and a number of others around the country. But it wouldn't have happened without the support of Europol and other partners in 19 countries. And in addition to the FBI obtaining enough evidence for search

warrants and indictments in the U.S., we shared information with our foreign partners to help them make their own cases against the Darkode perpetrators residing in their jurisdictions.

Operation Shrouded Horizon is a prime example of why the most effective way to combat cyber crime—which operates globally—is a law enforcement response that also transcends national borders.

Resources

- Major Computer Hacking Forum Dismantled (https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/major-computer-hacking-forum-dismantled)
- Cyber Crime (https://www.fbi.gov/investigate/cyber)
- Operation Shrouded Horizon (https://www.fbi.gov/audio-repository/news-podcasts-thisweek-operation-shrouded-horizon.mp3/view)